UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

PETER LAZAR and SHEBA KHAN, *on behalf of themselves and all others similarly situated,*

Plaintiffs,

-against-

INTERNATIONAL SHOPPES, LLC and DIPLOMATIC DUTY FREE SHOPS OF NEW YORK, INC.,

Defendants.

----------X

MEMORANDUM OF DECISION AND ORDER

Civil Action
No. 24-4170 (GRB) (SIL)

GARY R. BROWN, United States District Judge:

Plaintiffs Peter Lazar and Sheba Khan (collectively "plaintiffs") commenced this putative class action against International Shoppes, LLC and Diplomatic Duty Free Shops of New York, Inc. (collectively "defendants") following a November 2023 third-party cyberattack against defendants that resulted in a data breach ("Data Breach"). Plaintiffs sue for (1) negligence, (2) breach of implied contract, (3) unjust enrichment, (4) breach of fiduciary duty, (5) violations of New York General Business Law ("GBL") § 349, and (6) declaratory judgment. *See* Amended Class Action Complaint, Docket Entry ("DE") 15 ¶¶ 118-97. Presently before the Court is defendants' motion to dismiss this action pursuant to Federal Rule of Civil Procedure 12(b)(6). For the reasons stated herein, the motion is GRANTED in part and DENIED in part.

Factual Background

Data Breach

Defendants operate duty-free retail stores in U.S. airports. DE 15 ¶ 2. As part of their

operations, defendants receive and maintain personally identifiable information ("PII") and protected health information ("PHI") of thousands of current and former employees, vendors, and customers, who include consumers, diplomats, and foreign military personnel. *Id.* ¶ 17. As asserted in their privacy policy, which is available on their website, defendants "implement[] strict security measures to protect the information … from access by unauthorized persons and against unlawful processing, accidental loss, destruction and damage." *Id.* ¶ 21.

On November 16, 2023 hackers from LockBit, a Russian cybercriminal group, attacked defendants' computer systems, which resulted in the Data Breach. *Id.* ¶¶ 22-23, 25, 43. According to the Federal Bureau of Investigation ("FBI") and U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), LockBit "employ[s] double extortion by first encrypting victim data and then exfiltrating that data while threatening to post that stolen data on leak sites." *Id.* ¶ 45. Here, the LockBit attackers exfiltrated sensitive data of current and former employees, vendors, visitors, and customers, which included names, addresses, birth dates, Social Security numbers, driver's license and passport information, financial account numbers, and health information. *Id.* ¶¶ 26-30, 42, 48. LockBit threatened to publish the stolen PII and PHI by May 21, 2024 unless defendants paid a ransom. *Id.* ¶ 48. Defendants did not notify plaintiffs of the Data Breach until February 8, 2024, 69 days after the attack. *Id.* ¶ 34.

Plaintiffs' Experiences

Plaintiffs Lazar and Khan allege that the Data Breach resulted in the exposure of their PII and PHI, *id.* ¶ 57-58, and that cybercriminals have already published—or will imminently publish—such sensitive information, *id.* ¶¶ 49, 59.

Defendants employed Mr. Lazar from 2006 until 2014. *Id.* ¶ 50. During his employment, Mr. Lazar also purchased items as a customer. *Id.* Mr. Lazar alleges that as a

result of the Data Breach, he faces the risk of identity theft and has incurred over $2,000 in fraudulent debit card charges. *Id.* ¶ 9. Mr. Lazar has also suffered from a spike in spam text messages and phone calls following the Data Breach. *Id.* ¶ 66. And his credit score dropped 34 points during November 2023, the month of the Data Breach. *Id.* ¶ 67. Mr. Lazar spent weeks communicating with his bank so that his fraudulent charges could be reimbursed; even though he was eventually reimbursed, he was unable to access those funds during the intervening time. *Id.* ¶¶ 62-63. And as a result of the Data Breach, Mr. Lazar has been forced to spend time monitoring his accounts to protect against identity theft. *Id.* ¶ 65.

Defendants employed Ms. Khan from 2018 until 2019. *Id.* ¶ 51. She also purchased items as a customer during that time. *Id.* Ms. Khan alleges that as a result of the Data Breach, she has incurred unauthorized credit and debit card charges. *Id.* ¶ 70. She has dealt with a spike in spam text messages and phone calls, as well as "attempts of identity theft and misuse of her social security number." *Id.* ¶ 72. Ms. Khan "has spent—and will continue to spend—significant time and effort contacting her financial institutions, replacing her debit and credit cards due to unauthorized charges, and monitoring her accounts to protect against identity theft." *Id.* ¶ 73.

Plaintiffs filed suit on behalf of a putative class on December 12, 2024 for (1) negligence; (2) breach of implied contract; (3) unjust enrichment; (4) breach of fiduciary duty; (5) violation of GBL § 349; and (6) declaratory judgment. *See id.* ¶¶ 118-97. Defendants filed a motion to dismiss all six claims pursuant to Federal Rule of Civil Procedure 12(b)(6). *See* DE 19.

Discussion

Standard of Review

The Court has applied the well-trodden standard, recently discussed in *Potter v. Inc. Vill. of Ocean Beach*, No. 23-CV-6456 (GRB)(ARL), 2024 WL 3344041, at *4 (E.D.N.Y. July 9, 2024), *aff'd*, No. 24-2033-CV, 2025 WL 1077405 (2d Cir. Apr. 10, 2025), in deciding a defendant's motion to dismiss. In sum, assuming the allegations of the complaint to be true and drawing inferences in favor of the plaintiffs, the factual matters asserted must be facially plausible and support the propounded claims.

Negligence

Under New York state law, a plaintiff suing for negligence must prove: "(1) the existence of a duty on defendant's part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof." *Borley v. United States*, 22 F.4th 75, 79 (2d Cir. 2021).

On the first prong, "employers have a duty to take reasonable measures to protect PII that they require from their employees" regardless of whether a data breach is a result of a third party's action, because "attempts by hackers to access PII stored in an internal network are highly foreseeable." *In re Waste Mgmt. Data Breach Litig.*, No. 21-CV-6147 (DLC), 2022 WL 561734, at *4 (S.D.N.Y. Feb. 24, 2022). "Employees ordinarily have no means to protect that information in the hands of the employer, nor is withholding their PII a realistic option," making employers "best positioned to avoid the harm in question." *Sackin v. TransPerfect Global, Inc.*, 278 F.Supp.3d 739, 748 (S.D.N.Y. 2017) (quoting *In re New York City Asbestos Litig.*, 27 N.Y.3d 765, 59 N.E.3d 458, 469 (2016)). Companies also owe customers a duty to safeguard their PII. *Toretto v. Donnelley Fin. Sols., Inc.*, 583 F. Supp. 3d 570, 593 (S.D.N.Y. 2022) (holding that an investor relations firm had a duty to protect consumers' PII from a data breach). A company's privacy policy can evidence a duty to safeguard PII and PHI. *Id.* at 593-94.

On the second prong, Second Circuit courts have held that a company's failure to take

reasonable measures to protect PII can constitute a breach. *See In re Canon U.S.A. Data Breach Litig.*, No. 20-CV-6239 (AMD)(SJB), 2022 WL 22248656, at *7-8 (E.D.N.Y. Mar. 15, 2022) (denying dismissal where company failed to comply with industry standards for safekeeping of plaintiffs' PII)*; In re GEICO Customer Data Breach Litig.*, No. 21-CV-2210 (KAM)(SJB), 2023 WL 4778646, at *15 (E.D.N.Y. July 21, 2023), *report and recommendation adopted*, 691 F. Supp. 3d 624 (E.D.N.Y. 2023) ("Plaintiffs sufficiently allege [defendant] breached this duty by failing to adopt, implement, and maintain fair, reasonable, or adequate security measures despite reasonably foreseeable internal and external risks") (citation omitted)).

And for the third prong, injuries can include time and money spent attempting to mitigate fraud, "ongoing, imminent, and impending threat of identity theft crimes," and "decreased credit scores and ratings." *In re GE/CBPS Data Breach Litig.*, 2021 WL 340637, at *9 (S.D.N.Y. Aug. 4, 2021). At the motion to dismiss stage, disclosure of a plaintiff's PII which precedes fraud or identity theft is sufficient to infer that the injury is traceable to the disclosure. *In re GEICO*, 2023 WL 4778646, at *15.

Here, plaintiffs have pleaded all three elements of a negligence claim. First, as both an employer and a business serving customers, defendants had a duty to take reasonable measures to protect plaintiffs' PII and PHI. Defendants acknowledged this duty in their online privacy statement by assuring that they "implement[] strict security measures to protect the information [employees and customers] provide [] from access by unauthorized persons and against unlawful processing, accidental loss, destruction and damage." DE 15 ¶ 21.

Second, plaintiffs have stated a plausible claim that defendants breached their duty to safeguard PII and PHI by failing to follow industry standards for cybersecurity such as training employees, installing anti-virus and anti-malware software, requiring multi-factor authentication,

and limiting which employees can access sensitive data. *Id.* ¶ 100-103.[1] Plaintiffs have also pleaded that defendants failed to act reasonably by waiting 69 days until after discovering the Data Breach to notify the class, thereby depriving employees and consumers of an opportunity to mitigate damages. *Id.* ¶ 35.

And third, plaintiffs have sufficiently pleaded an injury as a result of the unauthorized disclosure of their PII and PHI. In November 2023, the same month as the Data Breach, Mr. Lazar's credit score dropped by 34 points. *Id.* ¶ 67. In April 2024, he incurred two fraudulent debit card charges for over $2,000. *Id.* ¶ 61. As a result of the Data Breach, Mr. Lazar has spent "significant time and effort monitoring his accounts to protect himself from identity theft." *Id.* ¶ 65. Ms. Kahn has incurred unauthorized credit and debit card charges following the Data Breach and has spent "significant time and effort contacting her financial institutions, replacing her debit and credit cards due to unauthorized charges, and monitoring her accounts to protect against identity theft." *Id.* ¶¶ 70, 73. At the pleading stage, plaintiffs have adequately stated their injuries resulting from the Data Breach.

Accordingly, the Court denies defendants' motion to dismiss the negligence claim.

Breach of Implied Contract

"A contract implied in fact may result as an inference from the facts and circumstances of the case … and is derived from the presumed intention of the parties as indicated by their conduct." *Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of NJ., Inc.*, 448 F.3d 573,

[1] Plaintiffs allege that defendants' failure to undertake reasonable security protections violates Section 5 of the FTCA and HIPAA. DE 15 ¶¶ 98-99, 104-07. While plaintiff does not allege negligence *per se*, any such claim would fail, because neither statute provides a private right of action. *In re Canon U.S.A. Data Breach Litig.*, 2022 WL 22248656, at *9 ("[A] negligence *per se* claim is not available under New York law because Section 5 does not provide a private right of action.").

582 (2d Cir. 2006) (citation omitted). The elements of a breach of implied contract are the same as for a traditional breach of contract claim and require: "(1) the existence of a contract, (2) performance by the party seeking recovery, (3) breach by the other party, and (4) damages suffered as a result of the breach." *Zam & Zam Super Mkt., LLC v. Ignite Payments, LLC*, 736 Fed. Appx. 274, 276 (2d Cir. 2018).

In a data breach case, a company's representations about its privacy protections in internal documents can create an implied in fact contract with employees and customers. *See Sackin*, 278 F. Supp. 3d at 750-51; *Wallace v. Health Quest Sys.*, Inc., 2021 WL 1109727, at *10 (S.D.N.Y. Mar. 23, 2021) ("The terms of the Notice of Privacy Practices, along with the notices defendant posted on its website, support an inference that [the defendant] intended to be bound by its obligation to safeguard plaintiffs' Private Information"). To plead that a defendant breached an implied contract, a plaintiff must "allege that [the defendant] failed to reasonably safeguard [] data." *In re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *5.

Here, plaintiffs have pleaded that an implied contract existed, which defendants breached by failing to adequately safeguard employees' and customers' data. Defendants' representation in their online privacy statement that they would protect plaintiffs' data is sufficient to create an implied contract. DE 15 ¶ 21. Employees and customers were required to provide their PII and PHI to defendants in exchange for employment, products, or services and "reasonably understood that a portion of the funds they paid … would be used to pay for adequate cybersecurity measures." *Id.* ¶ 145-46. Defendants breached the implied contract by failing to take reasonable measures to safeguard consumer and employee data. As discussed *supra*, defendants failed to follow industry standards regarding password protection, installation of anti-virus and anti-malware software, and use of multi-factor authentication. *Id.* ¶¶ 100-03. As a

result, plaintiffs suffered injuries in the form of decreased credit ratings, unauthorized expenses, and costs incurred while mitigating the fallout from the Data Breach. *Id.* ¶¶ 61-73.

Accordingly, the Court denies defendants' motion to dismiss the implied breach of contract claim.

Unjust Enrichment

To state a claim for unjust enrichment, a plaintiff must plausibly allege "(1) that the defendant benefitted; (2) at the plaintiff's expense; and (3) that equity and good conscience require restitution." *Myun-Uk Choi v. Tower Research Capital LLC*, 890 F.3d 60, 69 (2d Cir. 2018). An unjust enrichment claim "is not available where it simply duplicates, or replaces, a conventional contract or tort claim." *Corsello v. Verizon N.Y., Inc.*, 18 N.Y.3d 777, 790 (2012). Only "where a bona fide dispute exists as to the existence of the contract, the plaintiff may proceed on both breach of contract and quasi-contract theories." *Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J., Inc.*, 448 F.3d 573, 587 (2d Cir. 2006) (quoting *Nakamura v. Fuji*, 253 A.D.2d 387, 677 N.Y.S.2d 113, 116 (1st Dep't 1998)).

Here, the unjust enrichment claim is duplicative of the breach of implied contract claim. Defendants do not dispute the existence of a contract; rather, they argue that plaintiff does not adequately plead breach, causation, and damages. DE 19 at 20-21. Thus, there is no dispute that defendants' privacy policy created an implied contract.

Accordingly, the Court grants defendants' motion to dismiss the unjust enrichment claim.

Breach of Fiduciary Duty

"To state a breach of fiduciary duty claim under New York law, a plaintiff must plead: (i) the existence of a fiduciary duty; (ii) a knowing breach of that duty; and (iii) damages resulting therefrom." *Johnson v. Nextel Commc'ns, Inc.*, 660 F.3d 131, 138 (2d Cir. 2011). "A fiduciary

relationship exists when one person is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation." *Spinelli v. Nat'l Football League*, 903 F.3d 185, 207 (2d Cir. 2018) (quoting *Flickinger v. Harold C. Brown & Co., Inc.*, 947 F.2d 595, 599 (2d Cir. 1991)). However, employers are not fiduciaries of their employees. *See Kamdem-Ouaffo v. Balchem Corp.*, 2018 WL 4386092, at *18 (S.D.N.Y. Sept. 14, 2018) ("[A]n employer does not owe a fiduciary duty to its employees simply by virtue of the employment relationship."); *Rather v. CBS Corp.*, 886 N.Y.S.2d 121, 125 (1st Dep't 2009).

Here, there is no indication that defendants were fiduciaries of plaintiffs. The mere fact that plaintiffs were employees was not sufficient to create a fiduciary relationship. As for consumer plaintiffs, the fact that defendants stored their PII and PHI does not mean that defendants were "under a duty to act for or to give advice for the[ir] benefit." *Spinelli*, 903 F.3d at 207.

Accordingly, the Court grants defendants' motion to dismiss the breach of fiduciary duty claim.

GBL § 349

New York law authorizes a private right of action against "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service." N.Y. Gen. Bus. Law § 349(a). To maintain a cause of action under § 349, "a plaintiff must allege that a defendant has engaged in [i] consumer oriented conduct that is [ii] materially misleading and that [iii] plaintiff suffered injury as a result of the allegedly deceptive act or practice." *Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015). A complaint must make "reference to the specific acts, representations and/or omissions that [the plaintiff] claims are deceptive" and allege "why these acts were deceptive." *Horowitz v. Stryker Corp.*, 613 F. Supp. 2d 271, 287

(E.D.N.Y. 2009). A "deceptive act or practice" is a "representation or omission" that is "likely to mislead a reasonable consumer acting reasonably under the circumstances." *Stutman v. Chem. Bank*, 95 N.Y.2d 24, 29 (2000). Importantly, "[s]ection 349 does not create a free-floating obligation on all custodians of assets to safeguard those assets. The law guards against deception. Protection against the theft of assets … must be found, if at all, in other bodies of law." *Yuille v. Uphold HQ Inc.*, 686 F. Supp. 3d 323, 349 (S.D.N.Y. 2023).

Here, plaintiffs have not identified a "deceptive act or practice." *Stutman*, 95 N.Y.2d at 29. Plaintiffs point to defendants' privacy policy in which they tout their "strict security measures" and promise to "do [their] best to protect [plaintiffs' and class members'] personal information." DE 17 at 22; DE 15 ¶ 22. However, this statement "cannot be read to provide an assurance that there would be no circumstances under which [defendants' data] security systems would fail or that [their] accounts would be invulnerable to third-party attacks." *Yuille*, 686 F. Supp. 3d at 346. At this stage, the issue is not whether defendants have made a misleading statement, but rather whether they acted reasonably in protecting plaintiffs' data. The Court has addressed such claims in its discussion, *supra*, of plaintiffs' negligence and breach of implied contract claims.

Because plaintiffs do not allege that defendants made a misleading statement, the Court grants defendants' motion to dismiss the GBL § 349 claim.

Declaratory Judgment

"The Declaratory Judgment Act, 28 U.S.C. § 2201, does not create an independent cause of action." *Rand v. Travelers Indem. Co.*, 637 F. Supp. 3d 55, 72 (S.D.N.Y. 2022). "Its operation is procedural only – to provide a form of relief previously unavailable. Therefore, a court may only enter a declaratory judgment in favor of a party who has a substantive claim of

right to such relief." *In re Joint E. & S. Dist. Asbestos Litig.*, 14 F.3d 726, 731 (2d Cir. 1993). Declaratory relief must be forward looking and address the possibility that a plaintiff may face future harm from a defendant's act or omission. *See In re Unite Here Data Sec. Incident Litig.*, No. 24-CV-1565 (JSR), 2024 WL 3413942, at *16 (S.D.N.Y. July 15, 2024) (finding allegations of "continued inadequacy" in security measures sufficient to support a declaratory judgment claim).

Because plaintiffs' negligence and breach of implied contract claims survive, declaratory relief is not a standalone claim. Additionally, declaratory relief could prevent future harm by requiring defendants to exercise reasonable care in protecting PII and PHI of employees and customers. Plaintiffs have alleged that defendants' security measures remain inadequate, DE 15 ¶ 191, and that plaintiffs have "a continuing interest in ensuring that their PII/PHI, which … remains backed up in Defendants' possession, is protected and safeguarded against further breaches," *id.* ¶ 80.

Accordingly, plaintiffs' declaratory judgment claim survives.

Conclusion

For the reasons set forth herein, the Court denies defendants' motion to dismiss the negligence, breach of implied contract, and declaratory judgment claims and grants defendants' motion to dismiss the unjust enrichment, breach of fiduciary duty, and GBL § 349 claims.

SO ORDERED.

Dated: Central Islip, New York
May 22, 2025

/s/ Gary R. Brown
GARY R. BROWN
United States District Judge